

# Qualys WAS 4.8 New Features

We are pleased to announce Qualys Web Application Scanning 4.8 (WAS) featuring quick and easy vulnerability retest functionality, without having to launch a full scan as well as the ability to customize the severity of findings to meet your business needs.

## Feature Highlights:

- **Vulnerability Retest Functionality**
- **Vulnerability Severity Customization for Findings**

## Other Features and Changes:

- **Enhanced Display for Severity Level Text with Severity Icon**
- **Enhanced Reporting Detail for Function**
- **WAS Module Global Settings Support**

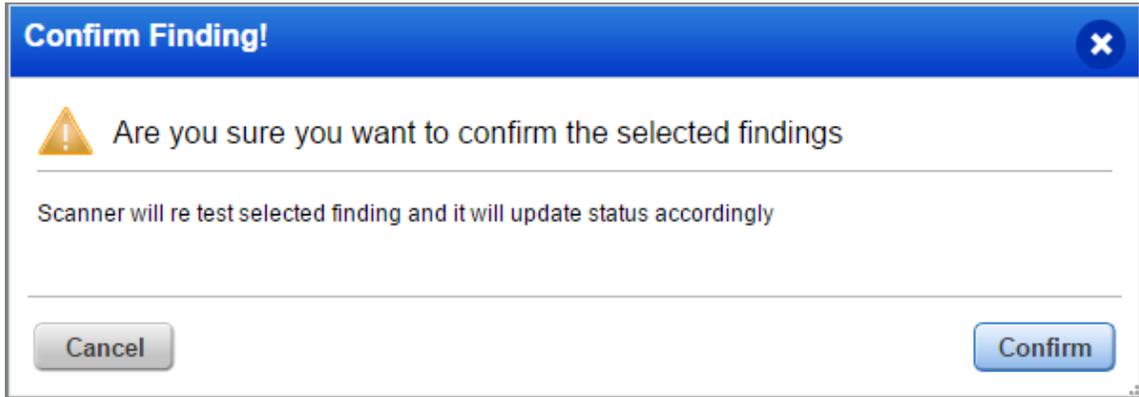
## Vulnerability Retest Functionality

Customers can now quickly retest vulnerability findings individually in WAS without launching another full scan. Within the Detections Tab, “Retest” will launch a scan to test the selected finding. Only potential vulnerabilities, confirmed vulnerabilities and sensitive contents are available for retest.



Severity	ID	Description	URL	Quick Actions	Created	Count	Severity Icon
New	150124	Clickjacking - Framable Page	http://funkytown.vuln.qa.qualys.com/cassum/	View	May 2016	0	Red
New	150085	Slow HTTP POST vulnerability	http://10.10.26.238/	Ignore Activate	May 2016	6	Yellow
New	150079	Slow HTTP headers vulnerability	http://10.10.26.238/	Install Patch Remove Patch	May 2016	6	Yellow
-	150067	Links Discovered During User-Agent and Mobile Site Checks	http://10.10.26.238/	Retest Cancel Retest	May 2016	6	Blue

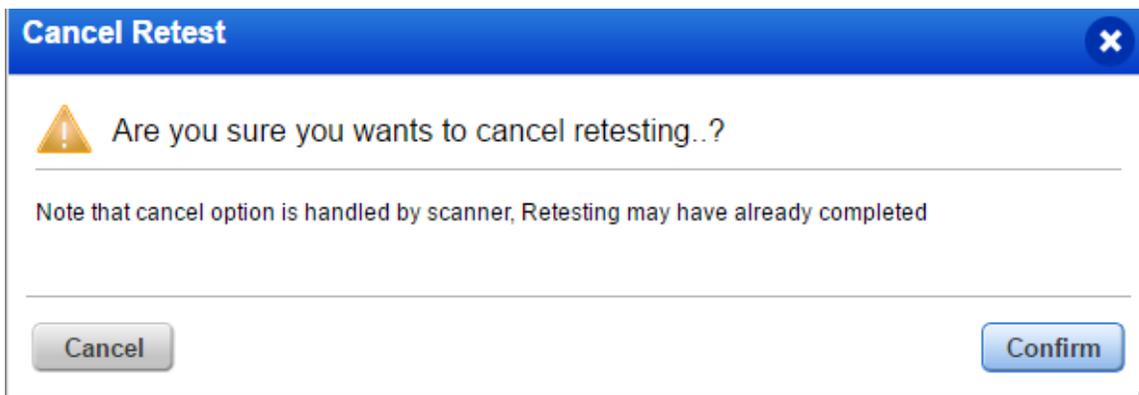
This will show a confirmation message for the retest action.



Users can also cancel the retest.



This will show a confirmation message to cancel the retest action.



Once a user launches the retest, and when finding is still under the test phase, the view panel will be updated as follows. There is also a cancel link on top of the right side so a user can click this link to cancel the retesting if desired.

**Vulnerability Details** ✕

! **This finding is currently being retested...** Cancel

Requested by: Snehil Mandavkar (quays\_sm)  
 Appliance: External  
 Date: 07 May 2016 5:41PM GMT+0530

This panel will be refreshed as soon as the check completes. Please wait for a moment...

■■■■■ 150060 HTTP Response Splitting Vulnerabilities
Active

URL: https://10.10.26.238/boq/parseAction.php

---

Finding #	119777	Web Application	Test App <iframe>
Patch #	-	Authentication	Not Used
Group	Information Disclosure		
CWE	CWE-113	First Time Detected	04 May 2016 2:40PM GMT+0530
OWASP	A5 Security Misconfiguration	Last Time Detected	04 May 2016 2:40PM GMT+0530
WASC	WASC-24 HTTP Request Splitting	Last Scan Date	04 May 2016 2:40PM GMT+0530
CVSS Base	7.5	CVSS Temporal	6.7
		Times Detected	1 View History...

Details Show

Detection Information

Parameter: It has been detected by exploiting the parameter **login** of the form located in URL **http://10.10.26.238/**  
 The payloads section will display a list of tests that show how the param could have been exploited to collect the information

Function: **Welcome**

Once the retest is finished the view dialog will be updated as follows:

Case 1: When Finding is fixed in retest. Status changed to Fixed.	Case 2: Finding is detected in retest. Status changed to Active.
<div style="background-color: #0056b3; color: white; padding: 5px;"> <b>Vulnerability Details</b> </div> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 5px;"> <div style="background-color: #e6f2ff; padding: 5px; border: 1px solid #add8e6;"> <span style="font-size: 1.2em; color: #0056b3;">!</span> <b>This finding is retested</b> </div> <div style="margin-top: 5px;"> <p>Requested by: Snehil Mandavkar (quays_sm)              Appliance: External              Date: 06 May 2016 11:34PM GMT+0530              Status: Finding has not been detected              Reason: Vulnerable URL cannot not be found anymore</p> </div> </div> <div style="margin-top: 10px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> <span style="color: #0056b3;">■■■■■ 150001 Reflected Cross-Site Scripting (XSS) Vulnerabilities</span> </div> <p>URL: https://10.10.26.238/boq/parseAction.php</p> </div>	<div style="background-color: #0056b3; color: white; padding: 5px;"> <b>Vulnerability Details</b> </div> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 5px;"> <div style="background-color: #e6f2ff; padding: 5px; border: 1px solid #add8e6;"> <span style="font-size: 1.2em; color: #0056b3;">!</span> <b>This finding is retested</b> </div> <div style="margin-top: 5px;"> <p>Requested by: Snehil Mandavkar (quays_sm)              Appliance: External              Date: 07 May 2016 3:51PM GMT+0530              Status: Finding has been detected              Reason: Finding could have been confirmed</p> </div> </div> <div style="margin-top: 10px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> <span style="color: #0056b3;">■■■■■ 150022 Syntax Error Occurred</span> </div> <p>URL: http://10.10.26.238/</p> </div>

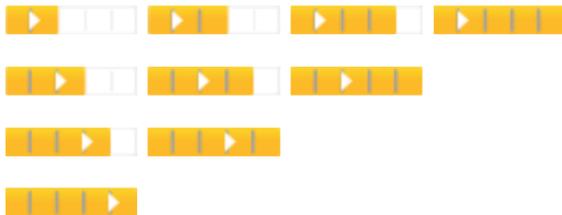
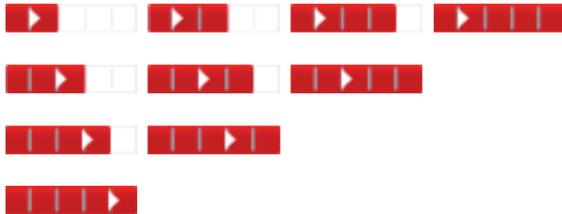
## Vulnerability Severity Customization for Findings

Users will now have the ability to customize the vulnerability severity of findings within Detections. This ability now pertains to vulnerability and sensitive content findings reported in their web applications. In addition, users will be able to specify comments along with any change made. Also, action logs shall be created to track changes made on the severity level. Visibility is available to show what was the Qualys severity level was prior to being updated. The severity level change shall have an impact on the dashboard stats, web application reports and when viewing detections.

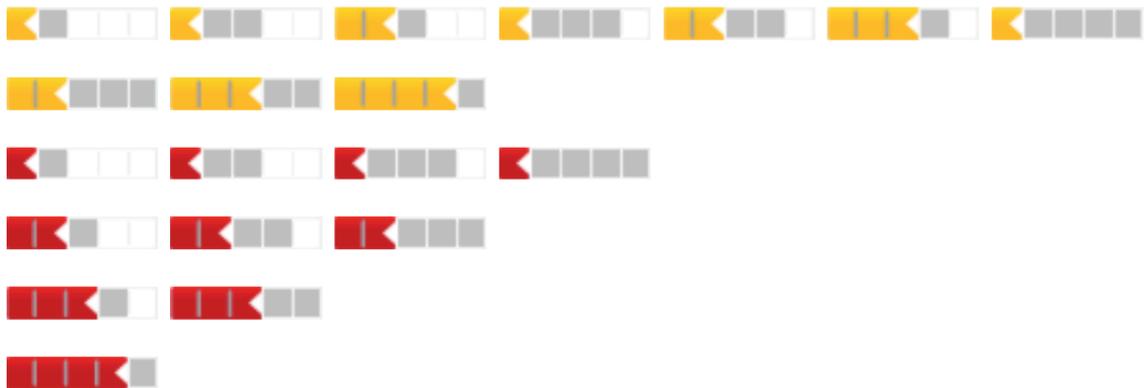
Each detection that had the severity level altered will use a different severity icon than standard:

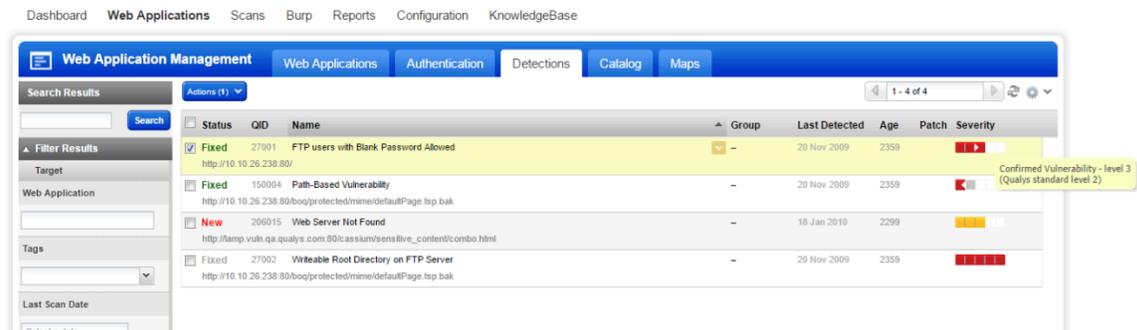
- The customized severity level will be displayed
- The Qualys standard level will be visible by using a small arrow to show which level the new value has been set from.

#### Increased severity examples



#### Decreased severity examples





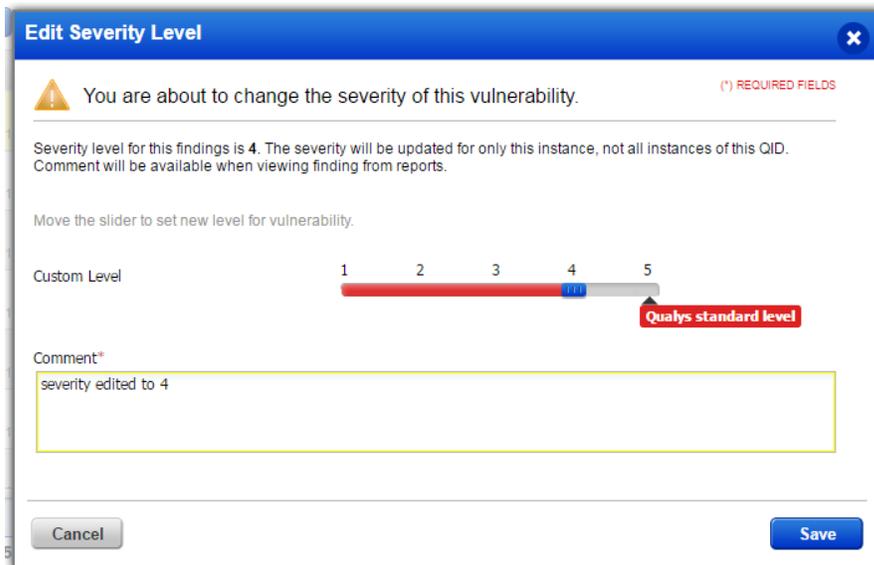
By moving the mouse over the icon, the user will also know what the Qualys standard level was prior to the change.

Qualys standard level - <severity level>

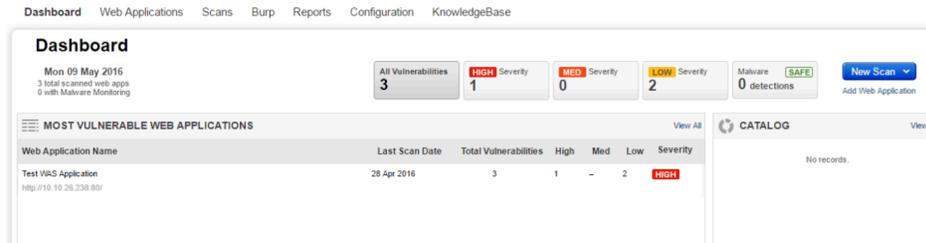
The same icon with tooltip will be available in the preview panel.

Edit Severity Dialog:

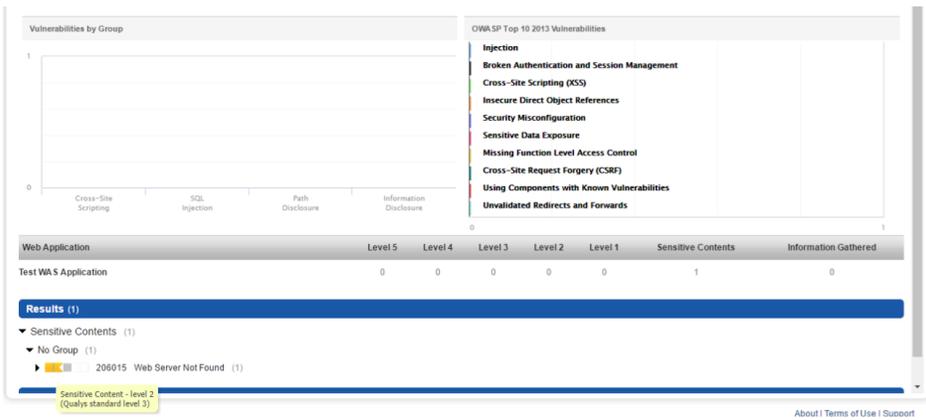
With this action, a dialog will open allowing the user to change the severity level on one or more findings. A mandatory comment is required by the user.



The severity level change shall have an impact on the entire WAS module, including dashboard stats, web application reports and when viewing detections.

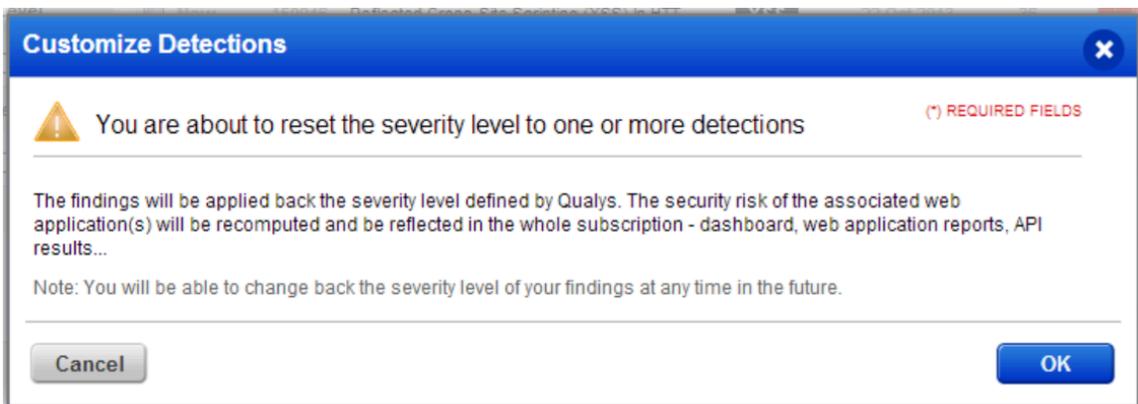


Dashboard stats



Restore Severity Level Dialog:

With this action, a dialog will open allowing a user to restore the default severity level set by Qualys on all selected findings. A confirmation dialog will be displayed, explaining to the user the impact of the change.



When the detection has been altered, the dialog will be refreshed to display an additional block notifying the user that the severity level for the detection has been either increased or decreased.

**Vulnerability Details** ✕

! **The severity level has been increased**
Restore Standard Level

Qualys Standard level: 2  
 Updated to level: 3  
 Updated by: Hamza BENZIOUCHE (quays\_hb)  
 Date: 06 May 2016 4:13PM GMT  
 Comment

Severity Level has been updated for finding from 2 to 3. updated

▶ 27001 FTP users with Blank Password Allowed
Install Patch Ignore Fixed

URL: http://10.10.26.238:80/

---

Finding #	647	Web Application	Test WAS Application
Patch #	-	Authentication	Not Used
Group	CWE -	First Time Detected	19 Nov 2009 6:30PM GMT
OWASP	-	Last Time Detected	20 Nov 2009 7:31PM GMT
WASC	-	Last Scan Date	12 Nov 2012 9:42PM GMT
CVSS Base	- CVSS Temporal -	Times Detected	1 View History...

Details Show

Detection Information
 

Parameter: No param has been required for detecting the information.

## Enhanced Display for Severity Level Text with Severity Icon

The Qualys severity name for each finding used to not be displayed. A small graphic image indicated the severity. The severity level names are defined in the appendix, but the severity name (5, 4, 3, 2, 1 –Confirmed, Potential) was never visible. Now the severity name as part of the severity information is displayed next to the severity graphic.

**WAS Scan Report**

■■■■ 150001 Reflected Cross-Site Scripting (XSS) Vulnerabilities

URL: https://10.10.26.238/?accountcorp=corporate

---

Finding #	1398012(38632593)	Severity	Confirmed Vulnerability - Level 5
Group	Cross-Site Scripting	First Time Detected	16 May 2016 02:54 GMT-0400
CWE	CWE-79	Last Time Detected	16 May 2016 02:54 GMT-0400
OWASP	A3 Cross-Site Scripting (XSS)	Last Time Tested	16 May 2016 02:54 GMT-0400
WASC	WASC-8 Cross-Site Scripting	Times Detected	1
CVSS Base	4.3 CVSS Temporal3.9		

## Enhanced Reporting Detail for Function

We previously introduced and started displaying Function with SOAP call fuzzing. Besides it's usefulness for ID calculation (to make different API calls unique) the element is now displayed in the UI for enhanced reporting detail.

**Vulnerability Details** ✕

**150046 Reflected Cross-Site Scripting In HTTP Header** Install Patch Ignore **Fixed**

URL: <https://10.10.26.238/boq/aboutus.php>

Finding #	1409794	Web Application	Copy of <script>alert()</script>
Patch #	-	Authentication	Not Used
Group	Cross-Site Scripting	First Time Detected	21 Oct 2015 12:30PM GMT
CWE	CWE-79	Last Time Detected	14 Dec 2015 12:30PM GMT
OWASP	A3 Cross-Site Scripting (XSS)	Last Scan Date	15 Dec 2015 12:30PM GMT
WASC	WASC-8 Cross-Site Scripting	Times Detected	7 View History...
CVSS Base	4.3	External References	-
CVSS Temporal	3.9		

Details Show

Detection Information

Parameter: It has been detected by exploiting the parameter `cookie2`  
The payloads section will display a list of tests that show how the param could have been exploited to collect the information

Function: **Welcome**

Access Path: Here is the path followed by the scanner to reach the exploitable URL:

```
http://10.10.26.238/
https://10.10.26.238/boq/parseAction.php
```

Payloads (3 instances) Show all payloads

#1 Request Show headers...

## WAS Module Global Settings Support

This new feature now allows Locale settings, Scan settings and Report settings to be configurable at the customer level in order to allow editing the default global settings by the manager.

We have added a new tab panel, 'Defaults' under the "Reports" section to add defaults for report settings:

**QUALYS GUARD** ENTERPRISE SUITE

Web Application Scanning Help Hamza BENZIOUCHE Log Out

Dashboard Web Applications Scans Burp **Reports** Configuration KnowledgeBase

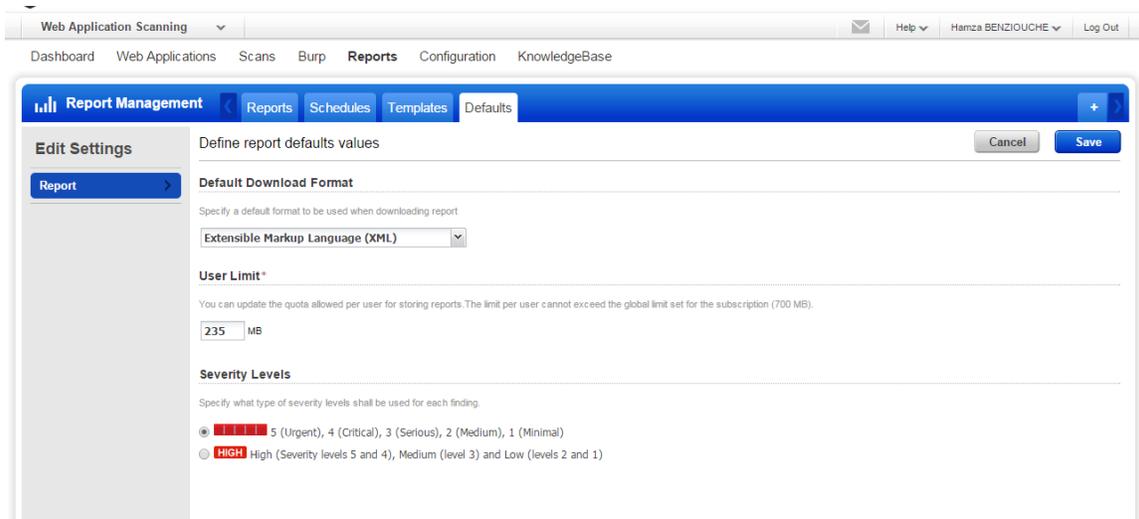
**Report Management** Reports Schedules Templates **Defaults**

**View Settings** Define report defaults values Edit

Report

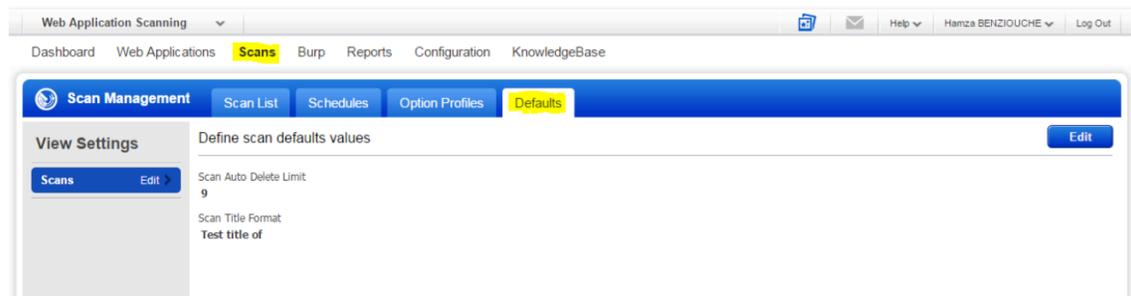
- Default Download Format
- Extensible Markup Language (XML)
- User Limit
- 235 MB
- Severity Levels
- numbers

Report Settings – View Mode

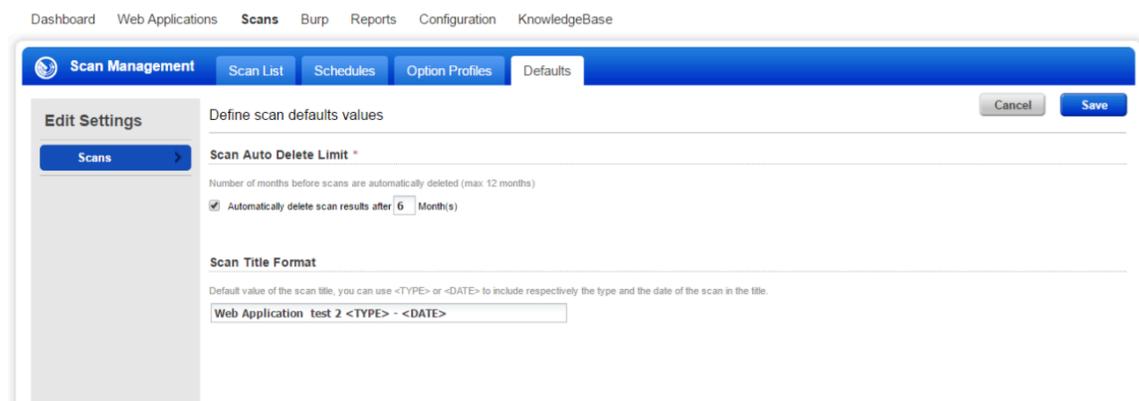


## Report Settings – Edit Mode

We added a new tab panel, 'Defaults' under "Scans" section to add defaults for scan settings:

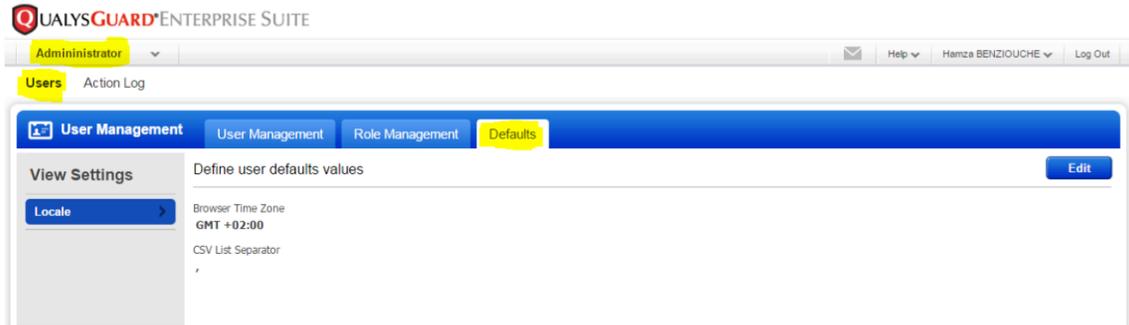


Scan Settings (View Mode)

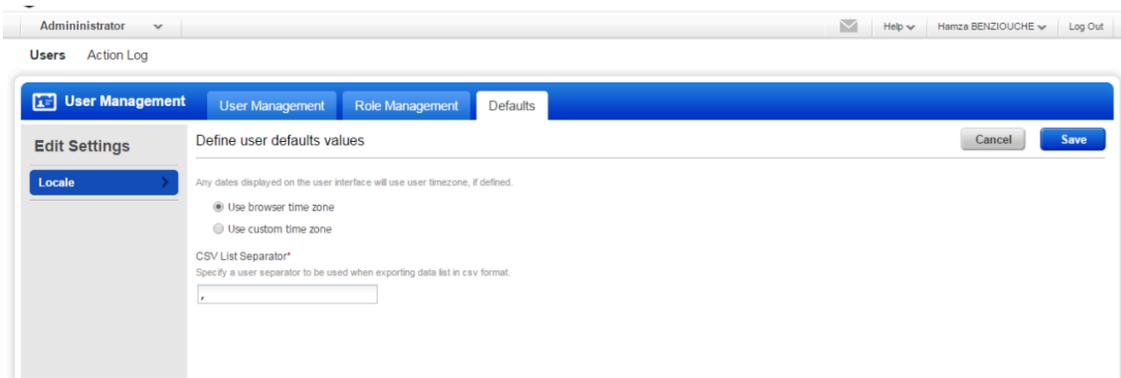


Scan settings - Edit Mode

We added a new tab panel, 'Defaults' under "Users" section in Admin module to add defaults for locale settings:



Locale Settings (View Mode)



Locale settings - Edit Mode